

ЗМІСТ

МЕТОДИ ТА МОДЕЛІ КРИПТОГРАФІЧНОГО АНАЛІЗУ ТА КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

<i>А.М. Олексійчук</i> Узагальнений диференціально-лінійний криптоаналіз блокових шифрів	5
<i>М.В. Єсіна, С.О. Кандій, Є.В. Острянська, І.Д. Горбенко</i> Генерація загальносистемних параметрів для схеми електронного підпису Rainbow для 384 та 512 біт безпеки	16
<i>І.Д. Горбенко, О.В. Потій, О.А. Замула</i> Концепція синтезу одного класу самосинхронізуючих дискретних сигналів	24
<i>В.І. Єсін, С.Г. Рассомахін, В.В. Вілігура</i> Аналіз формальних моделей забезпечення цілісності даних і їх застосовність для баз даних (рос.)	30
<i>М.В. Єсіна, Б.С. Шахов</i> Дослідження та аналіз реалізацій кандидатів другого раунду конкурсу NIST PQС, що орієнтовані на сімейства FPGA Xilinx	40
<i>С.О. Кандій, Г.А. Малєєва</i> Аналіз складності атак на мультіваріативні криптографічні перетворення з використанням алгебраїчної структури поля	59
<i>Є.В. Котух, О.В. Северинов, А.В. Власов, А.О. Теницька, Е. О. Зарудна</i> Деякі результати розробки схем криптографічних перетворень з використанням неабелевих груп (рос.)	66

РАДІОТЕХНІЧНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ ТА СИСТЕМИ

<i>Ю.Ю. Коляденко, О.В. Коляденко, Б.П. Муляр</i> Метод оптимізації розподілу частотного ресурсу з повторним використанням частот для систем когнітивного радіо	73
<i>М.О. Єрмошин, А.А. Побережний, О.С. Онопрієнко, М.П. Шурига</i> Архітектура сітьової бази знань складної системи воєнного призначення (англ.)	80
<i>О.В. Рязанцев, С.В. Марченко, М.В. Кулик</i> Про ефект Доплера в радіолокації (рос.)	93
<i>В.Г. Крижановський, С.П. Сергієнко, Д.В. Чернов, В.В. Крижановський</i> Підслуховування NFC-зв'язку на частотах вищих гармонік	99

ФІЗИКА ПРИЛАДІВ ТА СИСТЕМ

<i>В.М. Борцов, О.М. Лістратенко, М.А. Проценко, І.Т. Тимчук, О.В. Кравченко, О.В. Суддя, М.І. Сліпченко, Б.М. Чічков</i> Дисперсія наночасток в оптично прозорі полімерні матриці (рос.)	105
<i>Б.В. Жуков, А.В. Одновол</i> Контроль різниці рівнів рідини в суміжних резервуарах (рос.)	115

РАДІОТЕХНІЧНІ ПРИСТРОЇ ТА ЗАСОБИ ТЕЛЕКОМУНІКАЦІЙ

<i>Д.Г. Макаров, Д.В. Чернов, В.В. Крижановський, Ю.В. Рассохіна, В.Г. Крижановський, А. Гребенніков</i> Дослідження підсилювача класу E/F ₃ з паралельним контуром	120
--	-----

ПІДГОТОВКА СПЕЦІАЛІСТІВ В ОБЛАСТІ РАДІОТЕХНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ

<i>І.О. Мощенко, О.М. Нікітенко, Ю.В. Козлов</i> Можливості застосування СКМ Maple для дослідження законів розподілу випадкових величин (англ.)	128
---	-----

РЕФЕРАТИ	135
----------	-----

CONTENT

METHODS AND MODELS OF CRYPTOGRAPHIC ANALYSIS AND CRYPTOGRAPHIC TRANSFORMATIONS

<i>A.N. Alekseychuk</i> Generalized differential-linear cryptanalysis of block ciphers	5
<i>M.V. Yesina, S.O. Kandy, E.V. Ostryanska, I.D. Gorbenko</i> Generation of general system parameters for Rainbow electronic signature scheme for 384 and 512 security bits	16
<i>I.D. Gorbenko, O.V. Potii, A.A. Zamula</i> The concept of synthesis of one class of self-synchronizing discrete	24
<i>V.I. Yesin, S.G. Rassomakhin, V.V. Vilihura</i> Analysis of formal models for ensuring data integrity and their applicability to databases	30
<i>M.V. Yesina, B.S. Shahov</i> Research and analysis of implementations of the NIST PQC competition second round candidates focused on the Xilinx FPGA family	40
<i>S. Kandy, G. Maleeva</i> Analysis of the complexity of attacks on multivariate cryptographic transformations using algebraic field structure	59
<i>E.V. Kotukh, O.V. Severinov, A.V. Vlasov, A.O. Tenytska, E.O. Zarudna</i> Towards results of cryptographic transformations schemes development with application of nonabelian groups	66

RADIO AND TELECOMMUNICATION NETWORKS AND SYSTEMS

<i>Yu.Yu. Kolyadenko, O.B. Kolyadenko, B.P. Mulyar</i> Method for optimization of frequency resource allocation with frequency reuse for cognitive radio systems	73
<i>M. Yermoshyn, A. Poberezhnyi, O. Onopriyenko, M. Shuryha</i> Architecture of network knowledge base of a complex military system	80
<i>O.V. Ryazantsev, S.V. Marchenko, M.V. Kulik</i> On the Doppler effect in radar	93
<i>V.G. Kryzhanovskiy, S.P. Serhiienko, D.V. Chernov, V.V. Kryzhanovskiy</i> Listening to NFC at higher harmonic frequencies	99

PHYSICS OF INSTRUMENTS AND SYSTEMS

<i>V.M. Borshchov, O.M. Listratenko, M.A. Protsenko, I.T. Tymchuk, O.V. Kravchenko, O.V. Syddia, M.I. Slipchenko, B.M. Chichkov</i> Dispersion of nanoparticles in optically transparent polymer matrices	105
<i>B.V. Zhukov, A.V. Odnovol</i> Monitoring the difference in liquid levels in adjacent tanks	115

RADIO ENGINEERING DEVICES AND TELECOMMUNICATIONS MEANS

<i>D.G. Makarov, D.V. Chernov, V.V. Kryzhanovskiy, Yu.V. Rassokhina, V.G. Kryzhanovskiy, A. Grebennikov</i> Investigation into Class E/F3 with Parallel Network	120
---	-----

TRAINING OF SPECIALISTS IN THE FIELD OF RADIO AND TELECOMMUNICATIONS

<i>I. Moshchenko, O. Nikitenko, Yu.V. Kozlov</i> Possibility of using CMS Maple to study laws of distribution of random variables	128
---	-----

ABSTRACTS	135
-----------	-----